A story in ten parts

- Security threats and countermeasures
- Types of security
- Technologies for securing communication
- Identification and authentication
- Basic crypto
- Digital signatures and certificates
- Public Key Infrastructure (PKI) & the IETF's PKIX
- Authorization and the attribute certificate
- Legal aspects in commerce
- Threat and risk analysis

A few security terms

- *vulnerability* — a weakness that may be exploited
- *threat* — an event or action that may cause harm
- *risk* — the probability that a threat will exploit a vulnerability with resulting damage
- *countermeasure* — actions, e.g. technology or procedure, that reduce or eliminate vulnerability or threat

 hoytkesterson@earthlink.net

The need for security

- The business environment has changed
  - more sensitive information on-line intellectual property, organization strategy, operational information, personal information
    - » increased use of electronic communication by senior management
  - increased need for communication outside the organization
    - » business alliances (often with competitors)
    - » operational communication, e.g. Electronic Commerce, EDI
- The computing environment has changed
  - move to distributed computing, e.g. client/server
  - use of open, shared networks, e.g. the Internet, LANs, wireless
  - use of well known OSs, e.g. UNIX, NT
  - more information stored in remote departmental systems
- The threat has increased
  - attackers have inexpensive, but powerful, computers
  - available tools for examining & manipulating communication

 hoytkesterson@earthlink.net


The threats
IOU
$100
$1000
Line taps (sniffing)
Masquerades
Message alteration
Message replay
Unauthorized access to resources
Denial of Service
© Hoyt L. Kesterson II, Slide 7
hoytkesterson@earthlink.net


The LAN—an old–fashioned party line
© Hoyt L. Kesterson II, Slide 8
hoytkesterson@earthlink.net

The security countermeasures

- Is this the party to whom I am speaking?—authentication
  —don't increase logon complexity; do single logon
- Allow me to trust electronic documents—digital signature
- Don't let unauthorized people change my stuff—integrity
- Don't let unauthorized people see my stuff—confidentiality
- Don't let them do it and say they didn't—non-repudiation
- Don't let them stop my work—avoid denial of service
- Don't make me hire a bunch of people to do this—administration & audit

 hoytkesterson@earthlink.net

How do we do this?

- Physical security—keep unauthorized people away from your systems
- System security—protect the content of the system
- Communication security—protect what goes over the wire (or through the air)
- Develop a security policy
- Analyze the threats and and risks to your enterprise

 hoytkesterson@earthlink.net

System security

- Protect the content of the system
  - from users authorized to use the system
  - from unauthorized users
- Helps contain any breaches of communication security
- Accomplished with access control at the proper level of granularity
  - avoid the two class system, i.e. the normal user or the all powerful super-user
- Where a system cannot be physically secured, e.g. a laptop, consider encrypting the files on that system
- Correctness of implementation can be evaluated to *Common Criteria*
  - replaces the *Orange Book* trusted system evaluation, e.g. C2, B1
  - synthesis of US and European (IT/SEC) evaluation criteria

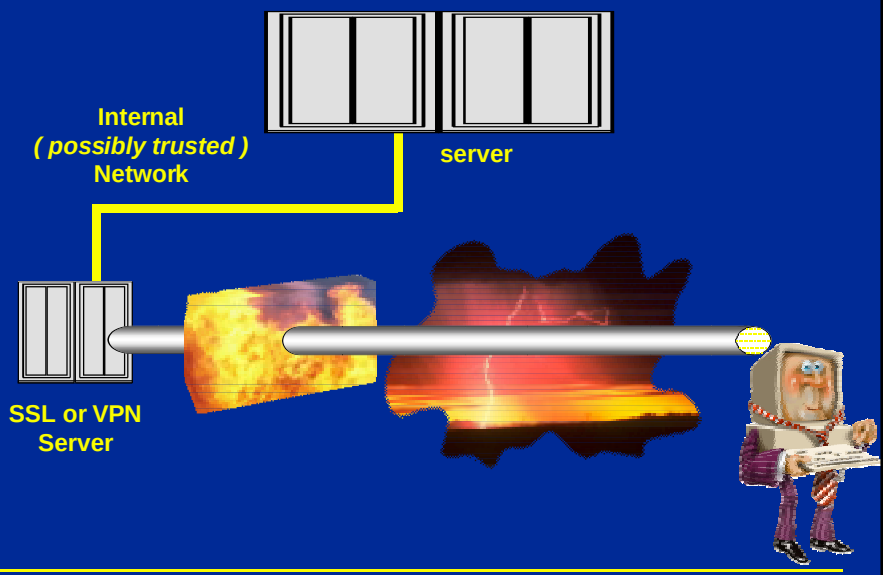
 hoytkesterson@earthlink.net

Communication security

- Firewalls are a good start but they may not be enough
  - often successful at blocking all external access
  - problems when some external users are permitted access
- Identify and authenticate users
  - manage your passwords properly
  - use one-time passwords, e.g. via token
  - cryptographic-based solution is strongest
- Protect the content of messages as they move between systems
  - confidentiality & integrity
  - secure the pipe or secure the message
    - » Kerberos, VPN, Secure Socket Layer (SSL), secure email
  - only cryptographic methods will work
- Cryptographic methods provide the best solutions

 hoytkesterson@earthlink.net

Secure communication pipe



 hoytkesterson@earthlink.net

Accessing a resource

- Identification
  - a name, human friendly if processed by people
  - unambiguous within the domain
  - often assigned by a registration authority
  - often hierarchical, e.g. Hoyt of Kesterson of Phoenix of Arizona
- Authentication
  - a proof of identity
  - ease of use, rigor, robustness, and resistance to attack vary
- Authorization
  - decision as to whether a resource can be accessed
  - criteria may include authenticated identity, time of day, location
  - variety of methods
    - » access control list
    - » sensitivity labels
    - » certificates

 hoytkesterson@earthlink.net

3 Factor Authentication

Something you know

Something you possess

Something you are

This concept came out of the *rainbow* series

- *A guide to understanding Identification and Authentication in Trusted Systems,* September 1991
- series produced by the National Computer Security Center

 hoytkesterson@earthlink.net

Something you know

- Information that only you, and possibly your intended correspondent, know
- Authenticator, PIN (personal identification number), password, passphrase
  - ideally processed only locally
    - » never transmitted across the network, or
    - » only transmitted once, e.g. one-time password, or
    - » protected in transmission
    - » held only in a transformed representation at the correspondent
  - sufficiently long and complex
    - » resist dictionary attack
    - » keep in memory
      - not too complex
      - avoid frequent change syndrome
- Cryptographic keying information

 hoytkesterson@earthlink.net

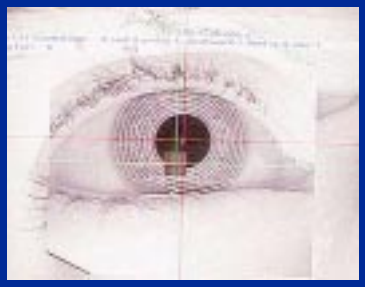
Something you have

- Proof that you possess a token
- Some tokens provide one-time passwords
  - stored list
  - challenge & response
  - time synchronized, e.g. SecurID
  - still may require something you know
- Smartcard
  - standalone, isolated system (trusted)
  - resistant to physical, electrical, and programmatic examination
  - can hold password or cryptographic info
  - can accept biometrics info, e.g. thumbprint
- Proximity detectors
  - system is locked when token, e.g. a badge, is removed to a certain distance

hoytkesterson@earthlink.net

Something you are

- A physical characteristic, a biometric
  - thumbprint
  - retinal scan
  - voice print
  - DNA? (you and your children can enter)
- Resist forgery, e.g. dead thumb, but recognize day to day variance
  - minimal number of false negatives
  - no false positives
- Speedy recognition
- Best used for local authentication
  - replayable across a network
  - read my lips, NOT a secret



hoytkesterson@earthlink.net

The crypto technology

- Encryption has been around for a long time
  - Caesar cipher substituted a character with the one three positions away
    - » A becomes D and Z becomes C
    - » exiib wkh ydpsluh vodbhu
  - subject to analysis and algorithm must be kept secret
- Goal is an mechanism where the algorithm is public and the result is resistant to analysis
- Three kinds of crypto mechanisms
  - one-way
  - symmetric
  - asymmetric
- Strength comes from the
  - robustness of the algorithm
  - correctness of the implementation
  - key space, e.g. the number of bits in the key

 hoytkesterson@earthlink.net

Symmetric Key

- T he same key is used to encrypt and decrypt the message
- Key distribution a problem
- Analysis forces frequent key change
- Relatively fast
- Examples are DES, triple DES, Motus, RC4, RC5, IDEA

 hoytkesterson@earthlink.net

Brute force attack

- Try all the keys
  - average is 50%
  - if key is derived from password, a dictionary attack may be more productive
- How many keys are there?
- The key space for 40 bits is a little over a trillion keys
- If one assumes that those keys would fit in a teaspoon and that half of them could be tried in one microsecond, then
  - the keys from the 56 bit key space (72 quadrillion) would fit in a child's swimming pool and half could be tried in .066 second
  - the keys from the 128 bit key space (BFN) would occupy the volume of the planet Earth and half could be examined in 9.8 quadrillion years.

 hoytkesterson@earthlink.net

Estimated time to break DES key

Type of attacker	Budget	40 bits	56 bits
Pedestrian hacker	$400	5 hours	38 years
Small business	$10K	12 minutes	556 days
Corporate department	$300K	24 seconds	19 days
Big company	$10M	7 seconds	13 hours
Intelligence agency	$300M	.0002 sec	12 seconds

- Study by leading cryptographers sponsored by Business Software Alliance in 1996
  - '97 cooperative search broke 40 bit RC5 in 3.5 hours; 56 bit DES in 127 days
  - EFF built $250K machine that in July 1998 cracked 56 bit DES in 56 hours
    - » see *Cracking DES* by the Electronic Frontier Foundation
  - at DES III Challenge in January 1999, a message encrypted with 56 bit DES was cracked in under 23 hours

 hoytkesterson@earthlink.net

Need a stronger key

- Clearly stronger encryption methods are needed
  - Triple DES may be stopgap
    - » encrypt with key 1, decrypt with key 2, and re-encrypt with key 1
    - » provides key space equivalent to 112 bits
- Replacement for the Data Encryption Standard, the Advanced Encryption Standard (AES)
  - minimum 128-bit block & 128-, 192-, and 256-bit key sizes
  - can be implemented in software and hardware (parallelism)
  - see http://csrc.nist.gov/encryption/aes/
  - round 1 produced five finalists from 15 candidates
    - » MARS, RC6, Rijndael, Serpent, Twofish
  - NIST selected Rijndael in October 2000
  - Federal Information Processing Standard (FIPS) by summer of 2001
    - » cryptographic module validation testing will be available
- Governments are concerned about increased use
  - export policy continually changing
  - some demand for control over domestic use

 hoytkesterson@earthlink.net

Asymmetric Key

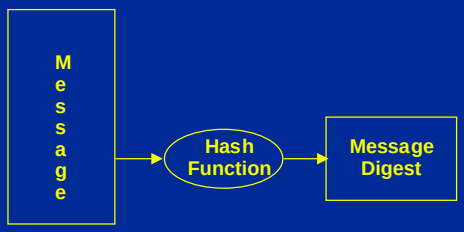
- One key is used to encrypt; another is used to decrypt
  - knowing one key does not give ability to determine other
  - one key is generally published—the public key
  - some methods allow the second key to verify but not to reverse the encryption
    - » US Digital Signature Standard
    - » typically slower for verifying a signature
- Used for digital signature
  - complex policy requirements can be supported, e.g. requester and approver, 3 out of 5
- Relatively slow
- Used for key exchange
- Examples are RSA, DSA, elliptic curve, shortest vector in a lattice
- Analysis of RSA requires solving factoring problem

 hoytkesterson@earthlink.net

Will elliptic curve succeed RSA?

- Smaller key size
  - 160 bits seems to offer same security as 1024 bit RSA or discrete logarithm crypto-system, e.g. DSA or El Gamal
  - attractive for a smartcard
- Analysis requires solving "elliptic curve discrete logarithm problem"
- Faster than corresponding discrete logarithm based systems such as DSA
- Faster than RSA in signing but slower in verifying
- Much more study needed

Signing a message

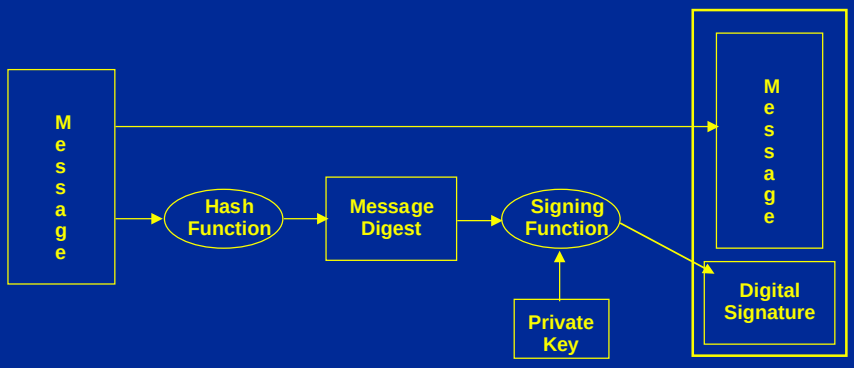


Hash functions

- Hash function is one-way
  - the message cannot be derived from the hash
  - computationally infeasible to construct two messages to produce the same digest
  - computationally infeasible to construct message to produce a given digest
- The result of a hash function is often called a message digest
- Encrypt message digest instead of message
  - keeps the message in clear plaintext
  - less processing to encrypt the short message digest
- MD5 still most widely used
  - 128 bit result
  - analysis has shown it may have some weaknesses
- Secure Hash Algorithm (SHA-1) is recommended
  - 160 bit result
  - half the performance of MD5

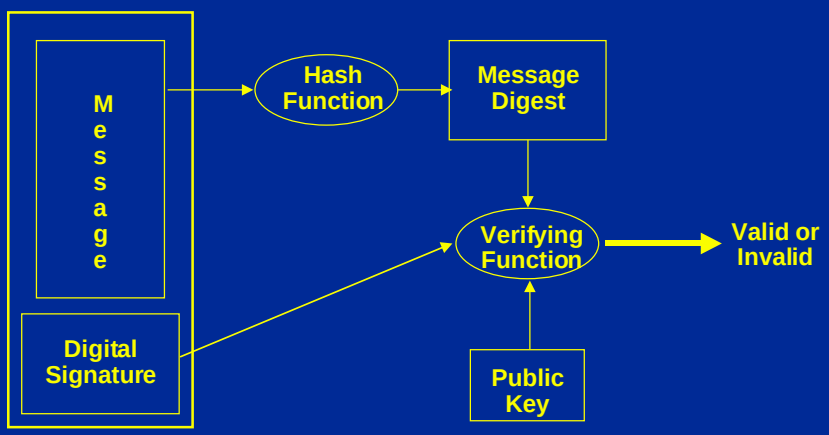
 hoytkesterson@earthlink.net

Signing a message



 hoytkesterson@earthlink.net

Verifying a signature



 hoytkesterson@earthlink.net

Digital Signature — enough?

- Gives confidence that the document originated from the owner of the public key and is unchanged
- Major question—who is the owner of that public key?
  - direct trust
    - » you acquire the public key in a direct communication with the owner
    - » the model for PGP (pretty good privacy)
    - » problems of scale and responsibility
  - hierarchical or chain of trust
    - » a trusted authority, the certification authority (CA), binds the user's identity to the public key in a signed certificate which is valid for a specified amount of time
    - » X.509 model

 hoytkesterson@earthlink.net

Quis custodiet ipsos custodes

- Why do you trust the authority?
- Its public key is in a certificate signed by a higher authority
- For example
  - the certificate for John, a purchasing agent for the Ford SUV Assembly Group, is signed by the Ford SUV Division certification authority
  - the certificate for the Ford SUV Division certification authority is signed by the Ford certification authority
  - the certificate for the Ford certification authority is signed by a well known national certification authority with well known public key
  - or Ford's certificate is trusted by the CA of Firestone. All these certificates can accompany the signed message — the certification path
    - » Ford and Firestone CAs issue cross certificates to each other

 hoytkesterson@earthlink.net

Certificate revocation

- The lifetime for a certificate can be long, e.g. a year
- What if the key is no longer good?
  - the key is compromised
  - the employee leaves the company
  - the employee's role changes
- Various approaches to determine validity; e.g.
  - the CA periodically issues a signed certificate revocation list
    - » CRL is published in a repository, e.g. a directory or web page
    - » forms are full, delta, distributed, indirect
  - use a protocol such as OCSP to immediately determine validity
- Risk influences method chosen; e.g.
  - purchase $5 movie ticket — none
  - purchase real estate worth $500,000 — CRL
  - purchase $1000 diamond bracelet — direct enquiry
- Certificate policy specifies rules
  - if *critical,* the relying party must follow those rules

 hoytkesterson@earthlink.net

Completely verifying a signature

Message	MD signed with user's private key

Certificate with user's public key	MD signed with CA x's private key

CA x's Certificate Revocation List	MD signed with CA x's private key

Certificate with CA x's public key	MD signed with CA y's private key

CA y's Certificate Revocation List	MD signed with CA y's private key

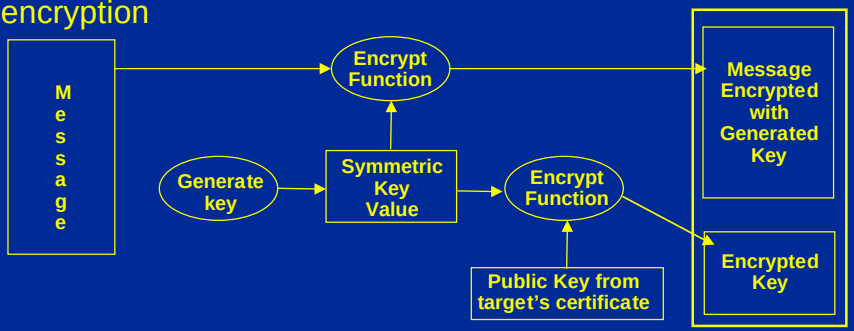
If the signed message digest does not match that generated for the received message or certificate, the message signature authentication fails

If the serial number of any of the certificates is listed, the message signature authentication fails

 hoytkesterson@earthlink.net

Encrypting a message

- Sender and receiver must agree on key
- One key exchange method uses reversible asymmetric encryption



- Other methods allow both users to generate the same key value, e.g. using each other's public key value
- As done for digital signature, the public key value is bound to the target in a certificate signed by a trusted authority

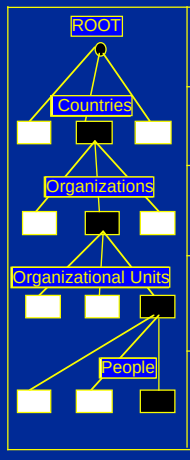
 hoytkesterson@earthlink.net

The Certificate specifies

- the subject's name as assigned by a naming authority (an X.500 distinguished name)
  - » other forms, e.g. RFC822 email, are allowed

 hoytkesterson@earthlink.net

Distinguished Names



RDN	Distinguished Name
{}	{}
C=UK	{C=UK}
O=Telecom	{C=UK, O=Telecom}
(OU=Sales, L=Ipswich)	{C=UK, O=Telecom, (OU=Sales, L=Ipswich)}
CN=Smith	{C=UK, O=Telecom, (OU=Sales, L=Ipswich), CN=Smith}

 hoytkesterson@earthlink.net

The Certificate specifies

- the subject's name as assigned by a naming authority (an X.500 distinguished name)
  - » other forms, e.g. RFC822 email, are allowed
- the subject's public key (and algorithm info)
- the validity period, I.e. the certificate can be used to validate a signature created during the interval of from the beginning date through the ending date
- a unique serial number for the certificate
- the name of the issuer—the certification authority
- signed by the certification authority
- key use—simple restrictions, e.g. use only for key exchange
- policy information—complex restrictions, e.g. use only in Visa credit transactions
- subject and issuer attributes—e.g. RFC822 name (e-mail) as alternate user name
- certification path constraints—e.g. accept only selected certificates from a CA
- see ftp://ftp.bull.com/pub/OSIdirectory for more details

 hoytkesterson@earthlink.net

Extensibility

- Need to add new information to certificate
  - by the ISO and ITU-T standards groups
  - by others, e.g. X9 banking standards, IETF
  - concern for proliferation of varying certificate definitions
- Extensibility mechanism defined
  - ignore undefined fields unless marked critical
    - » ASN.1 encoding enables this

Type	Length	Value

  - added to certificate definition
    - » version 3
  - added to CRL
    - » extension to the CRL list as a whole
    - » extension to the entry identifying a revoked certificate
    - » version 2

 hoytkesterson@earthlink.net

Public Key Infrastructure (PKI)

- Procedures and protocols needed to specify
  - parties and roles in the environment
    - » subscribers, relying parties, CAs, name registration authorities, repositories
  - commercial relationships (e.g. fees), responsibilities, and assumed liabilities of each of the parties;
  - protocol specifics such as
    - » encryption algorithms
    - » key sizes
    - » rules for key pair generation
    - » collection of subscriber information
    - » presenting public key and subscriber information to the CA in a secure and trusted manner
    - » certificate content, profile, including validity period
    - » authorization information in an attribute certificate
    - » delivering the certificate to the owner
    - » revocation mechanisms
    - » refresh mechanisms

 hoytkesterson@earthlink.net

PKI Policies

- How trust among parties certified by different CAs will be established
- Managing the invalidation of a certificate before its expiration date, i.e. revocation
  - reasons
    - » private key compromise
    - » subject leaving the company.
  - how a certificate owner requests revocation in a secure and trusted fashion
  - how and when a relying party determines the validity status of a certificate.
- Certificate Policy (CP) constrain how the certificates may be used
- Some confused people think a CP just specifies how a CA operates
  - CAs conform to a Certification Practice Statement (CPS)

 hoytkesterson@earthlink.net

Inter-domain Trust

- Inter-domain business relationships require trust that enables appropriate transactions to occur and prevents inappropriate transactions
- "Appropriate" depends on specific business relationship, and policies under which the transactions occur
- PKI supports business controls through constraints:
  - Specified by CAs in cross-certificates
  - Specified for relying parties at path validation
- Certification path processing includes processing of standardized constraints for business controls

 hoytkesterson@earthlink.net

Business controls in X.509

- Basic constraints extension
  - Restricts maximum path length
- Name constraints extension
  - Restricts trusted namespaces to certificates with subject names:
    - » Of specific nameforms (e.g. DN or rfc822Name)
    - » Within specified subtrees of those namespaces
    - » Outside unacceptable subtrees
- Certificate Policies extension
  - Restricts acceptable certificate policies
- Policy mapping extension
  - Enables equivalent policies to be considered acceptable
- Policy constraints extension
  - Restricts policy mapping and requires explicit policy identification
- Inhibit any policy extension
  - Prevents wildcarding of certificate policy

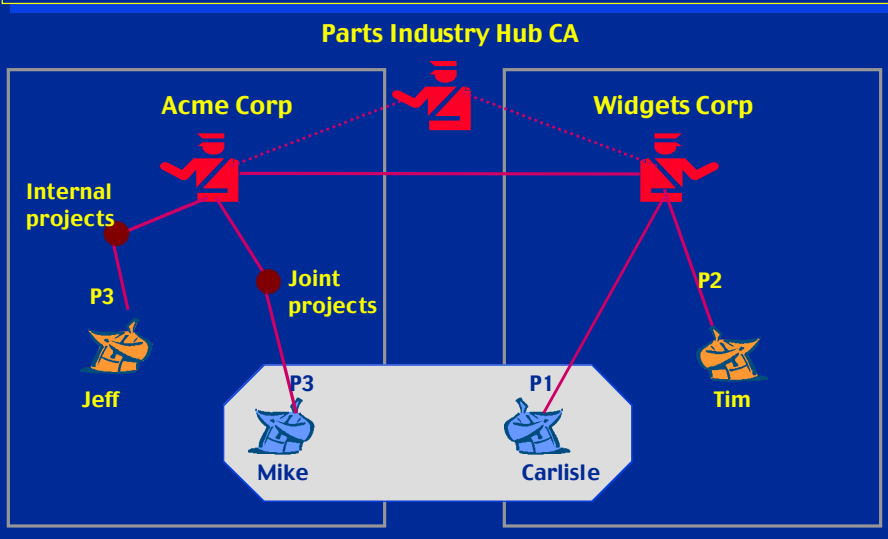
 hoytkesterson@earthlink.net

Business Controls Example

- Joint project involves subset of employees of Acme and Widgets
- Each company operates distinct PKI domain
- Acme uses names to identify its joint project employees
- Widgets uses certificate policies to identify its joint project employees

 hoytkesterson@earthlink.net

Joint Project Example



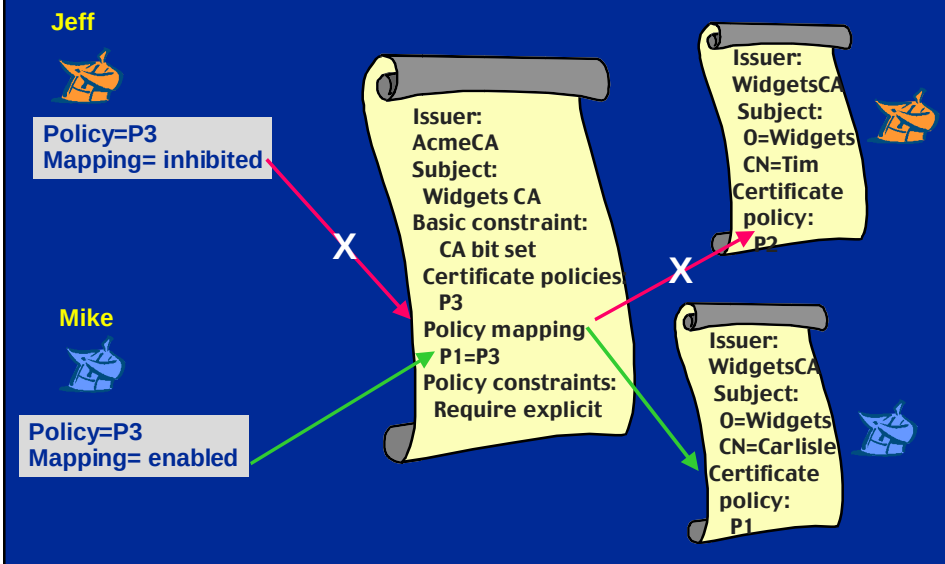
 hoytkesterson@earthlink.net

Sample Business Requirements

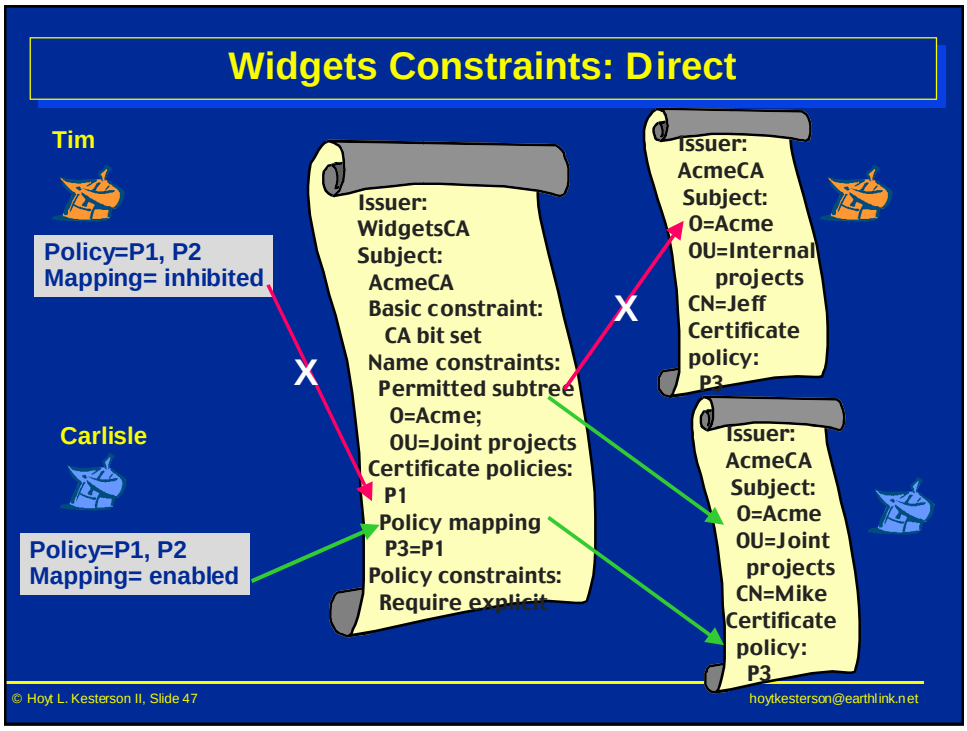
- All employees of Acme and Widgets must be able to trust certificates issued to other employees within their own organization
- In addition, joint project members in each organization need to be able to trust certificates issued to joint project members in the other organization
- No employee in either organization should trust certificates issued to employees in the other organization who are not working on the joint project

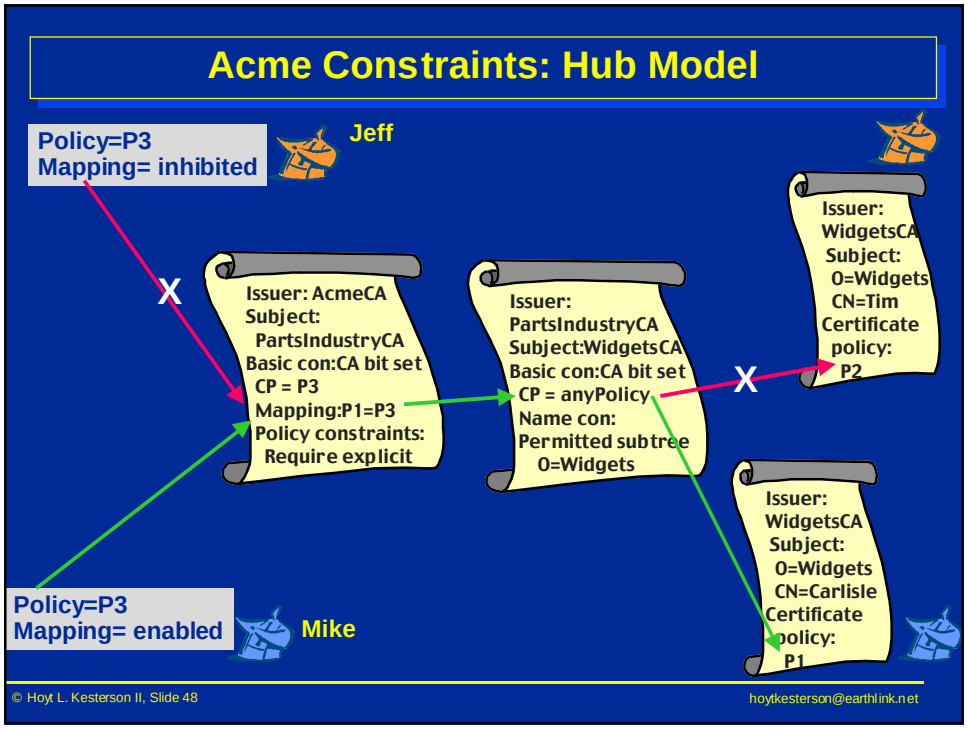
 hoytkesterson@earthlink.net

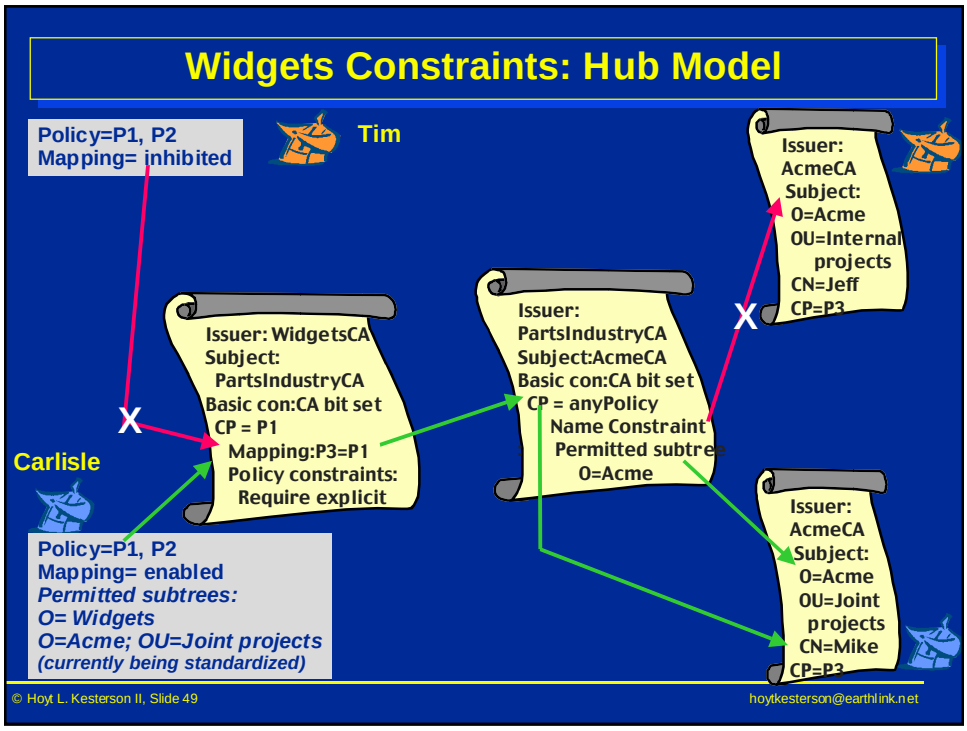
Acme Constraints: Direct

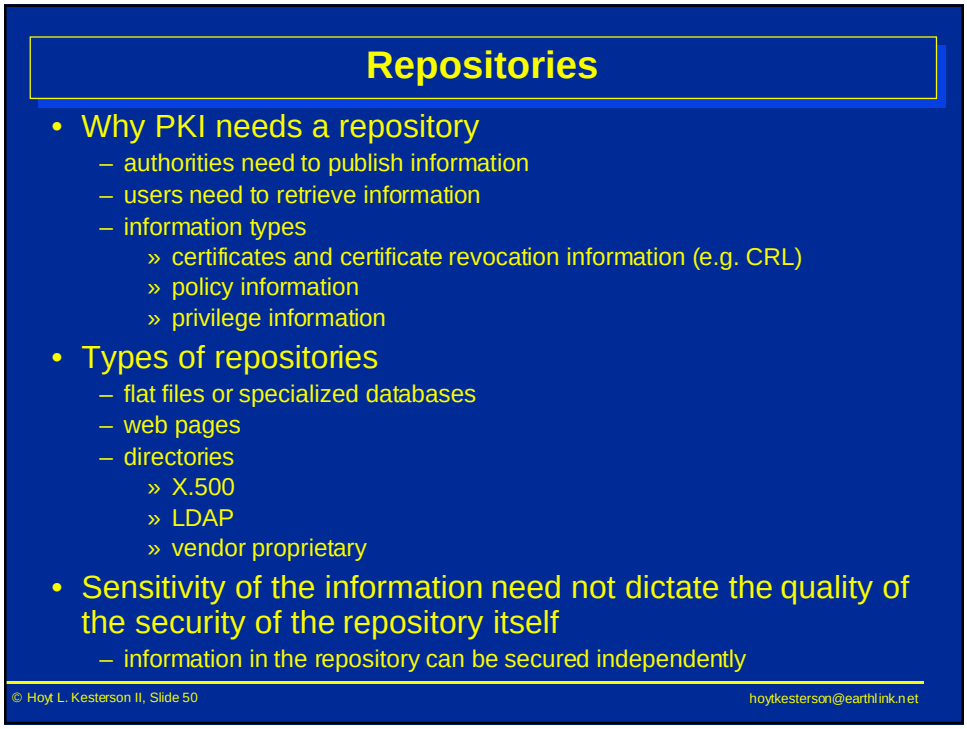


 hoytkesterson@earthlink.net


Widgets Constraints: Direct
Tim
Policy=P1, P2
Mapping= inhibited
Carlisle
Policy=P1, P2
Mapping= enabled
Issuer:
WidgetsCA
Subject:
AcmeCA
Basic constraint:
CA bit set
Name constraints:
Permitted subtree
O=Acme;
OU=Joint projects
Certificate policies:
P1
Policy mapping
P3=P1
Policy constraints:
Require explicit
Issuer:
AcmeCA
Subject:
O=Acme
OU=Internal
projects
CN=Jeff
Certificate
policy:
P3
Issuer:
AcmeCA
Subject:
O=Acme
OU=Joint
projects
CN=Mike
Certificate
policy:
P3
X
X
© Hoyt L. Kesterson II, Slide 47
hoytkesterson@earthlink.net


Acme Constraints: Hub Model
Policy=P3
Mapping= inhibited
Jeff
Policy=P3
Mapping= enabled
Mike
Issuer: AcmeCA
Subject:
PartsIndustryCA
Basic con:CA bit set
CP = P3
Mapping:P1=P3
Policy constraints:
Require explicit
Issuer:
PartsIndustryCA
Subject:WidgetsCA
Basic con:CA bit set
CP = anyPolicy
Name con:
Permitted subtree
O=Widgets
Issuer:
WidgetsCA
Subject:
O=Widgets
CN=Tim
Certificate
policy:
P2
Issuer:
WidgetsCA
Subject:
O=Widgets
CN=Carlisle
Certificate
policy:
P1
X
X
© Hoyt L. Kesterson II, Slide 48
hoytkesterson@earthlink.net


Widgets Constraints: Hub Model
Policy=P1, P2
Mapping= inhibited
Tim
Issuer: AcmeCA
Subject:
O=Acme
OU=Internal projects
CN=Jeff
CP=P3
Issuer: WidgetsCA
Subject:
PartsIndustryCA
Basic con:CA bit set
CP = P1
Mapping:P3=P1
Policy constraints:
Require explicit
Issuer:
PartsIndustryCA
Subject:AcmeCA
Basic con:CA bit set
CP = anyPolicy
Name Constraint
Permitted subtree
O=Acme
X
X
Carlisle
Policy=P1, P2
Mapping= enabled
Permitted subtrees:
O= Widgets
O=Acme; OU=Joint projects
(currently being standardized)
Issuer:
AcmeCA
Subject:
O=Acme
OU=Joint projects
CN=Mike
CP=P3
© Hoyt L. Kesterson II, Slide 49
hoytkesterson@earthlink.net

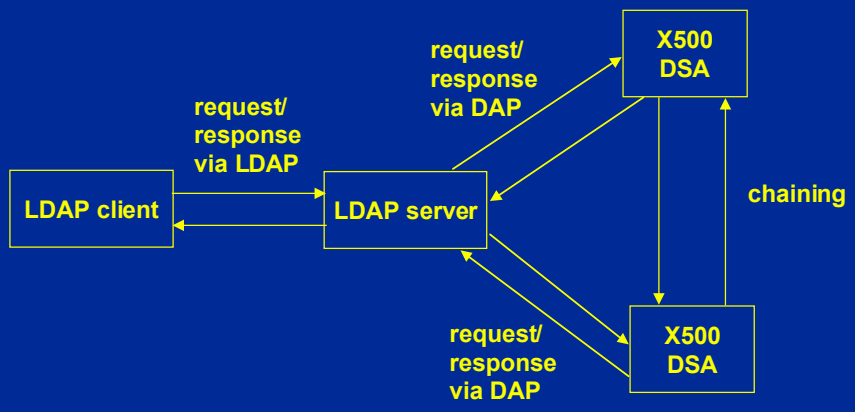

Repositories
• Why PKI needs a repository
– authorities need to publish information
– users need to retrieve information
– information types
» certificates and certificate revocation information (e.g. CRL)
» policy information
» privilege information
• Types of repositories
– flat files or specialized databases
– web pages
– directories
» X.500
» LDAP
» vendor proprietary
• Sensitivity of the information need not dictate the quality of the security of the repository itself
– information in the repository can be secured independently
© Hoyt L. Kesterson II, Slide 50
hoytkesterson@earthlink.net

Light Weight Directory Access Protocol (LDAP)

- Standardized by the IETF to access X.500 (and non-X.500) Directories
  - runs directly over TCP/IP
  - simplifies the X.500 model
    - » no read or list operations — use search instead
    - » no signing (secure the pipe instead, e.g. SSL)
  - uses string encodings for the ASN.1 structures
    - » version 3 uses UTF-8 encoding of UNICODE (BMP of 10646)
- Version 3, LDAPv3, will soon replace RFC 1779
  - referrals and URLs
  - security via underlying services
    - » SASL— Simple Authentication and Security Layer
    - » TLS—Transport Layer Security (subsumes SSL)
  - support for Unicode
  - extensibility

 hoytkesterson@earthlink.net

The LDAP model



 hoytkesterson@earthlink.net

The IETF Public Key Infrastructure—PKIX

- The Internet Engineering Task Force's PKIX working group has been developing specifications that;
  - specify a profile for the X.509 public key certificate and CRL;
  - specify a model and protocols for the management, e.g. requesting, of public key certificates;
  - specify transports to carry those protocols, e.g. TCP, HTTP;
  - specify an additional way to check the validity status of a certificate;
  - specify interfaces to repositories, e.g. LDAPv2;
  - specify the use of cryptographic mechanisms, e.g. Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and signatures;
  - Time stamping services and protocols; and
  - *more things than you have ever dreamt of*
- Pointers to the specifications can be found at http://www.imc.org/ietf-pkix/

 hoytkesterson@earthlink.net

Components of the PKIX model

- The end entity, i.e, the owner/subject of the certificate
  - generates key pair
  - request revocation
- The certification authority (CA)
  - collect and validate end entity information (unless RA present)
  - may generate key pair (particularly for encryption, e.g. key exchange)
  - issue the certificate
  - issue revocation status information
  - refresh certificates
  - archive key information
- The registration authority (RA)
  - collect and validate end entity information
  - name assignment
  - may generate key pair
  - may request revocation
  - often closer to the end entity
- The repository (LDAPv2)

 hoytkesterson@earthlink.net

PKIX certificate management protocol

- Minimal requirements for encryption for confidentiality
- The end entity gives the RA or CA
  - the public key and proof of possession of the private key
  - end entity information
  - if necessary, an unforgeable revocation request
- The RA can send the same information to the CA
- The CA sends the issued certificate to the RA/end entity
- The CA may publish in the repository
  - public key certificates, particularly for encryption for confidentiality
  - revocation information, CRLs
- A CA may communicate with another CA to issue cross certificates

 hoytkesterson@earthlink.net

On-line Certificate Status Protocol (OCSP)

- The requester knows the authority that can respond to OCSP requests
  - the authority that issued the certificate, the CA, may delegate the responsibility for responding to OCSP requests to another authority
- The request can ask the status of one or more certificates
- The response will contain
  - the status of each certificate
    - » good
    - » revoked
    - » unknown
  - date and time of
    - » the response was produced
    - » the time the status was known to be good
    - » optionally, when newer information about the status would be availble
  - digital signature of the OCSP responder

 hoytkesterson@earthlink.net

Time Stamping Service and Protocol

- A non-reputable transaction may require a record of the time and date of the transaction
- It may be that neither party will trust the other
- A trusted third party could provide a certified, i.e. a digitally signed, time stamp
- The requester
  - generates a hash of the message to be time stamped
  - sends it and other information, e.g. name, to the time stamp provider
- The time stamp service provider
  - checks the message for correctness, but
  - does not examine or log content
  - appends the date and time and a unique identifier to the hash
  - digitally signs the aggregate
  - transmit the timestamp to the requester
- The communication transport is assumed secure

 hoytkesterson@earthlink.net

Authentication & Authorization

- Public key certificates can be used to, e.g.:
  - support the digital signature on a document
    - » data origin authentication
  - support key exchange for encrypting data
  - authenticate the participants in a session
  - authenticate the initiator of a request
- An authenticated entity may be authorized to perform various functions
  - connect to a server
  - modify a file
- What the entity is permitted to do & to what, i.e. its privileges, can be obtained in a variety of ways, e.g.
  - the accessed object knows the entities that can access it and what they are permitted to do and when they can do it
  - the privileges of the accessing entity are provided to the accessed object

 hoytkesterson@earthlink.net

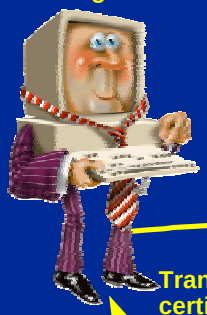
Authorization information in a certificate

- A certificate is an effective way to present privileges to the verifier for an object, e.g. to an access control decision function
- The certificate
  - will contain attributes that specify privileges
  - must not be modifiable or forgeable
  - digital signature provides integrity and proof of origin
- This is not a new concept
  - ECMA defined a Privilege Attribute Certificate (PAC)
  - supported in the Distributed Computing Environment (DCE)
  - Sesame enhanced the PAC with a digital signature
  - ANSI X9 defined an attribute certificate
- The X.509 public key certificate can also hold privileges, e.g. the clearance attribute

 hoytkesterson@earthlink.net

Source of Authority (SOA)

SOA, acting as an attribute Authority (AA), delegates privileges to holder by issuing a certified attribute



Transaction & attribute certificate presented to server

Verifier trusts SOA

Verifier validates path

 hoytkesterson@earthlink.net

An authorization scenario

Oracle DBs on the World Wide Wicket Company's servers have tables that identify which customers are consistently over 90 days late in making payment.

- Adhering to policy, the DB administrator configures the database such that only those entities with a role of *Grand Pooh-bah* can access the table
- J. Pierpont Finch needs to access that table but is denied since he is not a *Grand Pooh-bah* — therefore he either:
  - ✓ contacts the DB server administrator to become a *GP;* or,
  - ✓ contacts the security administrator who will create a certificate for him with a role attribute set to *GP* and stash it away for Ponty to retrieve
- Ponty appends that certificate to his next request
- The DB's access control function checks the certificate and, if valid, grants access to the restricted table

 hoytkesterson@earthlink.net

Advantages of the certificate method

- If done by the database administrator, each applicable DB must be configured
- In a centralized security management approach either
  - a centralized manager communicates through an agent to the DB system for the purpose of configuring security information for a user of that DB; or,
  - a centralized manager creates and signs a certificate specifying what privileges are assigned to the user
- The certificate approach has many advantages
  - application software need not supply access control configuration services for either agent or administrator access
  - agents do not have to be developed or deployed
  - a user who has been authorized to perform a function may, if permitted, delegate that privilege to someone else

 hoytkesterson@earthlink.net

The X.509 attribute

- An attribute is composed of
  - a unique name for the attribute using an Object ID
  - one or more values whose syntax is defined for the attribute
- The clearance attribute is a good example
- Each value of the clearance attribute will contain
  - the name of the security policy that defines the semantics of the clearance values, e.g. stating that *confidential* is higher than *restricted*
  - one or more classifications assigned to the holder of the certificate containing this attribute
    - » unmarked, unclassified, restricted, confidential, secret, top secret
  - optionally, one or more sub-categorizations of security within the classifications

 hoytkesterson@earthlink.net

Attributes in the X.509 public key certificate

- An X.509 public key certificate binds a public key to an entity
  - public key information
  - name of the entity owning the public/private key pair
  - public key certificate validity and revocation information
  - certificate policy
- The X.509 public key certificate can also hold authorization information in subjectDirectoryAttributes
- That authorization may be delegated, e.g. a certificate owner may act as a CA and Attribute Authority (AA)
  - either all privileges or no privileges must be delegated, i.e. no subsetting
- The authorization can be for a distributed application environment, e.g. a privilege attribute containing a role name that allows administrative access to all DBs in the enterprise

 hoytkesterson@earthlink.net

Public key or attribute certificate?

- An attribute is additional information about an entity
  - a role, e.g. purchasing agent
  - a label indicating that only documents with this sensitivity level or less can be accessed
  - a specific right, e.g. file write
- Public key certificates may contain attributes; but when
  - ✓the signing authority is different; or,
  - ✓validity period is different, e.g. very short; or,
  - ✓one doesn't want all privilege information to be exposed to all; or,
  - ✓there may be time period constraints, e.g. no weekend days; or,
  - ✓one or more privileges may be delegated; then,

  Attributes should be placed in a X.509 attribute certificate

 hoytkesterson@earthlink.net

Why delegation?

Ponty is going to climb trees to learn to be a team player. However, while he is gone someone must continue to monitor the 90 day information and, if necessary, contact the errant customer. Ponty assigns Rosemary Pilkington that task.

- Ponty could give Rosemary his private key and public key certificate
- Bad Boy! Bad Boy!
  - ☹ system cannot audit the identity of the initiator
  - ☹ Rosemary could decide to delegate the task to Bud Frump and pass on Ponty's information to Bud
  - ☹ it's impossible for Ponty to make his not-so-private key private again
  - ☹ Ponty just wanted to delegate the *GP* role but now Rosemary can do all that Ponty was authorized to do
- Ponty should have given Rosemary an attribute certificate containing only the *GP* role attribute.

 hoytkesterson@earthlink.net

The X.509 attribute certificate

The X.509 certificate is digitally signed by the issuer, i.e. the attribute authority (AA), and contains

- A version number (version 2 defined in 4th edition)
- The identity of the holder of the attribute certificate
- The identity of the issuer of the attribute certificate
- The identity of the algorithms used to sign the certificate
- A serial number, unique within the AA's domain, to unambiguously name the attribute certificate
- The period during which the certificate will be valid
- One or more attributes, e.g. role
- One or more extensions defined either
  - within the X.509 standard; or,
  - by other standardization organizations, e.g. financial, IETF
  - within the user community

 hoytkesterson@earthlink.net

The name of the attribute certificate holder

The name of the holder can come in several forms

- The identity of the holder's public key certificate, i.e. the issuer name & serial number of that public key certificate
  - the minimum information needed when the public key certificate accompanies the attribute certificate or is determinable within context
- The holder's name in one or more General Name forms
  - distinguished name, email address, URL, EDI Party Name, etc.
  - when by itself, the attribute certificate can be used with all the public key certificates containing this name
  - when accompanying a public key certificate issuer and serial number, it enables the verifier to associate a specific public key certificate
- The digest, i.e. hash, of the object holding the certificate
  - securely associates the certificate with an object
  - can specify the privileges of an initiator such as an applet
  - can specify the sensitivity, e.g. permissions, of the target object

 hoytkesterson@earthlink.net

The name of the attribute authority (AA)

- The identity of the AA that issued the attribute certificate
  - either one or more names for the issuer in General Name format; and/or,
  - the issuer and serial number of the certificate contain the public key associated with the private key used by the attribute authority to sign the issued attribute certificate
- That public key certificate may be that of the AA which is the Source of Authority (SOA) of the privileges contained in the issued attribute certificate.
  - this would be the normal case
- That public key certificate may be that of the entity to which privileges had been delegated by
  - the Source of Authority (SOA); or,
  - another AA
- An entity's right to delegate a privilege must be validated

 hoytkesterson@earthlink.net

Controlling delegation

- An extension in the attribute certificate indicates if the holder can delegate any privileges
- If delegation is allowed, delegation of the right to re-delegate the privilege can be limited to any depth
- The SOA issued Ponty an attribute certificate containing a role attribute of *Grand Pooh-bah*
- The basic constraints extension in Ponty's attribute certificate grants authority to delegate to a depth of one
- Ponty delegates to Rosemary by
  - constructing an attribute certificate with the *GP* role attribute
  - specifying Rosemary as the owner
  - setting basic constraints to not allow Rosemary to re-delegate
  - signing the certificate with the private key corresponding to the public key contained in the public key certificate identified in the attribute cert
- Rosemary cannot delegate the attribute certificate

 hoytkesterson@earthlink.net

Additional delegation restrictions

- Delegation can be restricted to entities whose public key certificate contain specific certificate policies
- Delegation can be restricted to entities whose names are within an identified name space
- For example, Ponty's attribute certificate may contain an extension stating that the first two relative distinguished names in the distinguished name of the owner of a delegated certificate must be "C = USA; O = World Wide Wicket Company"
  - Ponty cannot delegate a privilege to someone outside the company
- Or the constraint might be {C = USA; O = World Wide Wicket Company; CN = "Rosemary Pilkington"}
  - Ponty can only delegate to Rosemary

 hoytkesterson@earthlink.net

Revocation

- An attribute certificate may be revoked before it expires
  - a mechanism defined in X.509 is
    - » attribute certificate revocation list
    - » attribute authority revocation list
- Extensions provide the same choices as for a public key certificate, e.g. indirect, distribution point, delta
- It may be an acceptable risk to not check revocation status, e.g. when the attribute certificate's validity period is very short
  - an attribute certificate may contain a flag indicating no revocation information is available
- Checking the status of the public key certificate may subsume the status check of the attribute certificate

 hoytkesterson@earthlink.net

Temporal restrictions on use of a privilege

- An attribute certificate is valid only within the validity period specified within it
- One can further constrain when a privilege may be used using the time specification extension
  - absolute start or end times (e.g. 24:00 December 14, 1994);
  - specific time bands within the day (e.g. 09:00 to 17:00)
  - days within the week (e.g. Monday);
  - days within the month (e.g. the 10th; the 2nd last day, etc.);
  - months within the year (e.g. March);
  - a particular year (e.g. 1995);
  - weeks within the month (e.g. the second week);
  - periodic day or week (e.g. every 2nd week);
  - logical negatives (e.g. not Monday).

Privilege Management Infrastructure

- Needs support from a Public Key Infrastructure (PKI)
- Source of Authority (SOA) and Attribute Authority (AA)
- Attribute & privilege policy specification, perhaps formal
- Holders and repositories
- Initiators (claimants)
- Target objects
  - permissions are aspects whose use or evocation is governed (AKA object methods)
- Verifiers such as an access control decision function
- Profiles of acceptable extensions in attribute certificates
- Revocation policy
- Protocols to request and distribute attribute certificates, request revocation, and determine revocation status
- Severs issuing short or long-term attribute certificates

Enhancing Authorization

- Customers may not be ready for this stuff
  - single sign-on, encryption, stronger authentication
  - then centralized authorization
- As the requirement to secure every aspect of the enterprise grows we must move to more efficient ways to manage authorization
- A PMI using the X.509 attribute certificate can provide that efficiency

 hoytkesterson@earthlink.net

Communication security (a brief recapitulation)

- Assuming the server ensures that only authorized functions can be executed by the user, then:
  - the user must be properly authenticated;
  - the message must be protected from change while in transit;
  - it must be possible to conceal selected parts of the message while in transit; and,
  - the message shall only be processed once.
- Only encryption-based services can provide these functions
  - secured messages, e.g. via secured email, Secure Electronic Transaction (SET), secured EDI, and applets
  - secured sessions
  - secured transport, e.g. encrypted tunneling, Virtual Private Network (VPN)

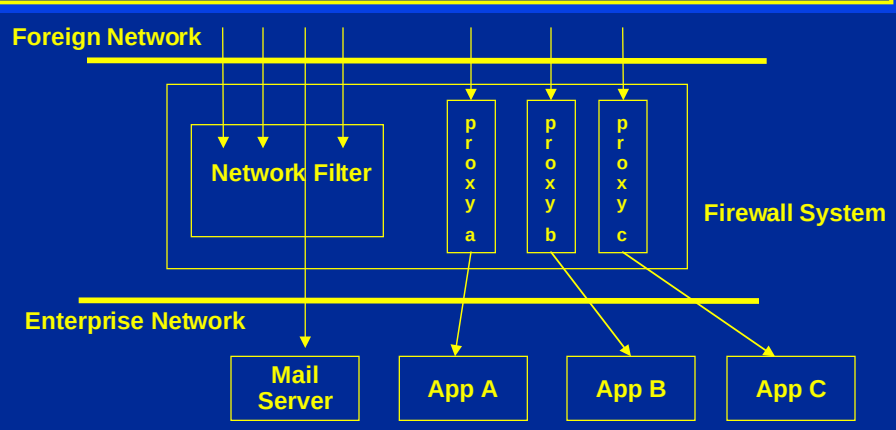
 hoytkesterson@earthlink.net

Deploying communication security

- Securing messages, e.g. by digital signatures, requires application change
  - messages are secure regardless of transport
  - since message integrity and proof of origin is persistent, non-repudiation of origin is achieved
- Securing the session typically requires modification of client and server
  - provides end to end security
  - authentication and data protection limited to duration of session
- Securing the transport will not impact applications
  - data protected only while in the secured pipe
  - security may not be provided end to end
- Securing the enterprise boundary
  - firewall proxy must be aligned with application
  - filtering is difficult if selected external users are privileged

 hoytkesterson@earthlink.net

The Firewall



- Filter decisions on source/target IP address and port
- Proxies determine if requests conform to security policies

 hoytkesterson@earthlink.net

Virtual Private Network

- VPNs offer a protected pipe between the communicating parties
  - In place transmission mode — only the data is encrypted but without change to packet size
  - Transport mode — only the data is encrypted but packet size changes
  - Encrypted tunnel mode — IP header and data are encrypted and a new IP header with the address of the target VPN node
- Most use SSLv3 but some are moving to IETF's TLS (Transport Layer Security)
- User authentication
  - password
  - multiple factor with token and/or biometrics
- Authorization, e.g. access control
  - what services and resources may be accessed

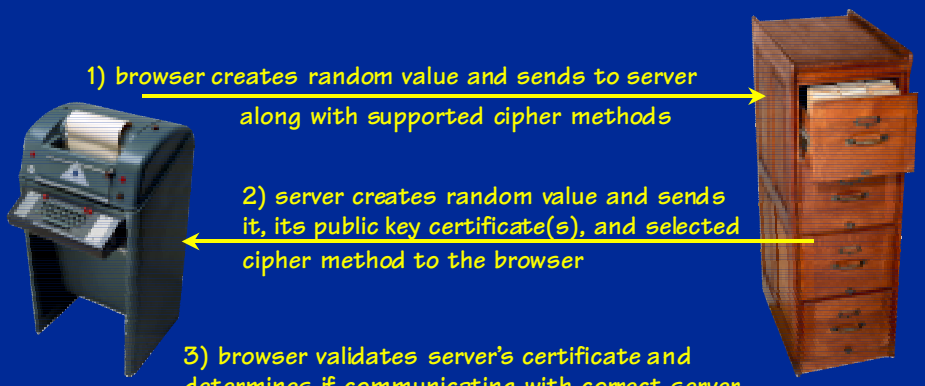
 hoytkesterson@earthlink.net

SSL—Secured Socket Layer

- Developed by Netscape
  - SSLv2 in 1994
  - SSLv3 in 1995 added
    - » certificate chains
    - » DSS and Diffie-Hellman (but not mandatory)
    - » closure handshake
- Uses a digital certificate to authenticate the server and determine a set of shared secret symmetric keys
- Handshake phase to agree on key values
- 40 bit or 128 bit RC4 and MD5
- Some alignment with TLS
  - DSS and Diffie-Hellman key exchange mandatory

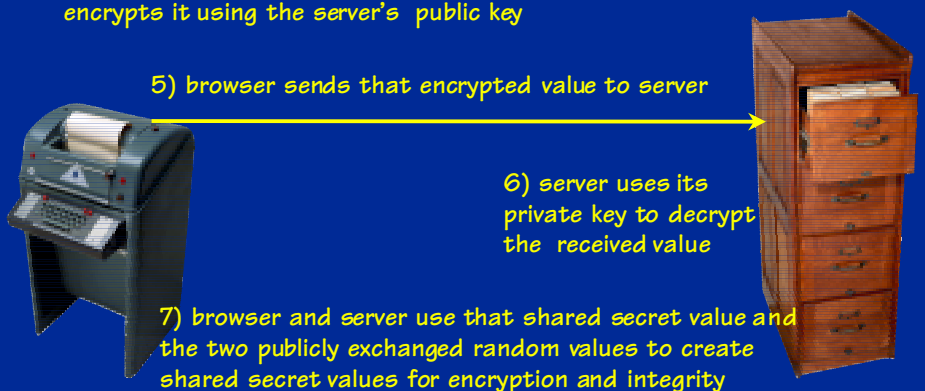
 hoytkesterson@earthlink.net

Using a certificate — SSL (PG-13)

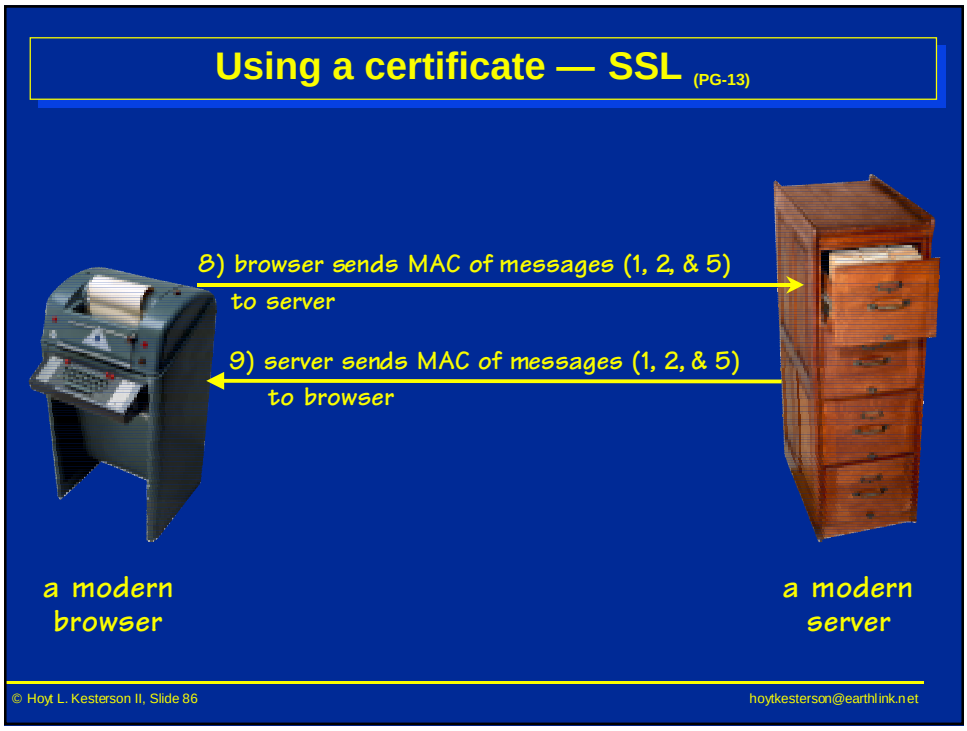


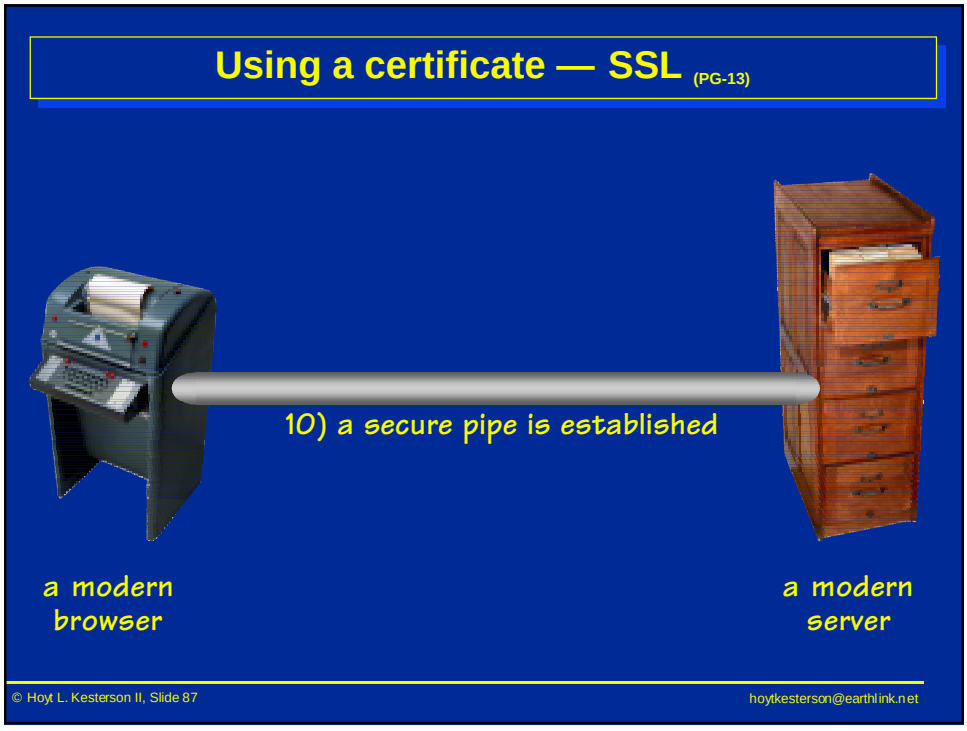
 hoytkesterson@earthlink.net

Using a certificate — SSL (PG-13)



 hoytkesterson@earthlink.net


Using a certificate — SSL (PG-13)
8) browser sends MAC of messages (1, 2, & 5) to server
9) server sends MAC of messages (1, 2, & 5) to browser
a modern browser
a modern server
© Hoyt L. Kesterson II, Slide 86
hoytkesterson@earthlink.net


Using a certificate — SSL (PG-13)
10) a secure pipe is established
a modern browser
a modern server
© Hoyt L. Kesterson II, Slide 87
hoytkesterson@earthlink.net

SSL — a little bit more

- Mutual authentication is an option
- Computed shared secrets
  - a symmetric key for each direction plus initialization vectors if needed
  - a key/value for each direction for computing a Message Authentication Code (MAC)
    - » HMAC (nested hashes) is used in TLS and a variant is used in SSL
  - Computation is different for SSL and TLS
- Messages are
  1) data fragmented if necessary
  2) data optionally compressed (no standardized routines)
  3) record header with message type and length, and SSL version
  3) record integrity and replay-prevention protected using HMAC
  4) data and MAC encrypted for confidentiality
- A security context can be maintained across sessions or used in multiple parallel sessions
- Security context can be changed during a session

 hoytkesterson@earthlink.net

IETF's Transport Layer Security Protocol, TLS

- TLS protects the integrity and "privacy" of data
  - TLS Record Protocol
    - » symmetric encryption using unique keys for each connection
      - can change algorithm and/or key during session
    - » message integrity check with a message authentication code, MAC
      - hash, e.g. SAH-1, plus secret
    - » encapsulates higher level protocols
  - TLS Handshake protocol
    - » entity authentication using asymmetric cryptography (optional)
    - » secure negotiation of a shared secret
      - secret used to compute master secret for encryption secret key, MAC secret, IV
  - may provide compression
- Based on SSLv3
  - differences are minor but TLS and SSL cannot interoperate
  - a TLS implementation can negotiate down to SSLv3
- Unlike IPSec, cannot prevent traffic analysis

 hoytkesterson@earthlink.net

IETF's IPSec

- Provide authentication, integrity, confidentiality, and anti-replay for the IP layer
  - And therefore for any higher layer protocol, e.g. TCP, UDP
- Authentication Header (AH)
  - data integrity and data origin authentication for a datagram
  - the data packet plus parts of the header are authenticated
- Encapsulating Security Payload (ESP)
  - authentication, integrity, confidentiality, anti-replay, anti-"traffic analysis"
  - does not authenticate the outer IP header however
  - can encrypt the original IP header and packet in "tunnel" mode
- Algorithms are DES, D-H, RSA, and SHA-1
- Security Association set up prior to data transfer
  - certificate based key exchange
    - » Internet Key Exchange (IKE), Internet Key Management Protocol (IKMP) based on ISAKMP and Oakley work
    - » plan to support key distribution centers, KDC (ala Kerberos)
  - encryption keys can be changed during the "session"

 hoytkesterson@earthlink.net

S/MIME
Secure Multipurpose Internet Mail Exchange

- Developed by IETF
- Uses digital signature to provide
  - message origin authentication
  - message integrity
  - non-repudiation of origin
  - uses SHA-1
- Encrypts for confidentiality
  - Uses 40 bit RC2 or triple DES
    - » mixture allowed when directed to multiple recipients
    - » key exchange with 512 to 1024 bit RSA
- Sender's email address must appear in the certificate's subjectAltName field
- Sender may include certificate chain and CRL

 hoytkesterson@earthlink.net

The applet—securing mobile code

- A message digest, e.g. MD5, of a file can be used to determine if the file has been corrupted
- Java uses code signing and the"sandbox" to provide enforcement rules
- Microsoft's ActiveX only uses code signing
  - Microsoft's Authenticode is for JAVA
- Unfortunately the certificate that would work for Netscape will not work for Explorer, and visa-versa
- There are trust issues
  - in June 1997 a developer distributed signed code that terminated Windows 95 and powered off the computer
    - » possessed a Individual Software Publisher Digital ID certificate
    - » certificate revoked but most code verification routines do not check the revocation status
  - Revocation status checking is still an issue with the two "Microsoft" certificates erroneously issued by Verisign in early 2001

 hoytkesterson@earthlink.net

EDI & Digital Signature

- Business to business, i.e. EDI, transactions moving to use of digital signatures
- ANSI X12 uses the X.509 certificate and PKI
- EDIFACT has designed an EDI specific
  - certificate structure
  - certificate management protocols, i.e. EDIFACT PKI
  - but can also use the X.509 certificate
- Has been incorporated into ISO standard 9735, application level syntax rules
- No policy support in EDIFACT certificate
  - Not a problem in closed trading partner relationship
    - » goal is security across open network, e.g. the Internet
    - » provides authentication, integrity, and confidentiality
  - If long range goal is Open EDI, use constraints must be specified
    - » law and regulation must provide contractual framework
    - » EDIFACT may extend its certificate to support policy

 hoytkesterson@earthlink.net

How can a smartcard help?

- A smartcard can give us some confidence that
  - private keys have been properly protected
  - the crypto functions are being performed properly
- The smartcard can hold the private key
  - act as a token for identification
  - augmented by other factors, e.g. fingerprint, password
  - the subscriber does not have to know the private key
  - mobility is supported without weakening security
  - the subscriber obligations are more easily met
- The smartcard can hold certificates and CRLs
  - both public key and attribute
- The smartcard can perform the crypto functions in a "trusted system" manner
  - the private key never leaves the smartcard
  - trypto functions cannot be circumvented or modified
- There are attacks, e.g. power differential

 hoytkesterson@earthlink.net

Key recovery—a prudent business practice

- Valid business requirement
- Critical business information may be unrecoverable if the encryption key becomes unavailable
  - employees forget!
  - employees become unavailable, e.g. ill, vacation, business travel
  - organizations need to be able to access encrypted information of terminated employees
- Employees may be improperly using organization resources
  - transferring information to unauthorized persons
  - operating unauthorized, and possibly criminal, venture
- Key recovery should allow access to
  - stored encrypted data
  - encrypted communication, e.g. email

 hoytkesterson@earthlink.net

Key recovery—possible roadblocks

- Concern about abuse by government agencies
  - these concerns should not block development of useful technology
  - strong laws should control access to this information
- Concern about acceptable key recovery center (KRC)
  - companies should be able to operate their own KRAs
- Concern about weakening protection
  - most concerns directed at large scale, centralized, government-approved KRCs
  - it is another point of attack
  - one must balance the risk resulting from a successful attack on the key recovery system with the risk of unrecoverable information

 hoytkesterson@earthlink.net

Proper implementation of key recovery

- Recognize that different types of information have different sensitivities
  - a doctor's business and billing information is less sensitive than the patient records
  - don't grant access to information without constraints, e.g. period of time
- Personal privacy a policy issue
  - explain key recovery possibilities and responsibilities to employees
  - should outside correspondents be apprised of key recovery possibilities?
- Ensure the facility cannot be abused
  - clearly specify when a key may be recovered
  - require the participation of more than one person and more than one organization to retrieve a key
- Document in a security policy

 hoytkesterson@earthlink.net

Security Policy statement

- Signals senior management's support
- Identifies the organization's information and resources that need to be protected
  - mandates the development of procedures to protect selected items
  - defines procedures to handle successful attacks
    - » evidence collecting
    - » guidelines for determining when to pursue civil or criminal prosecution
- States organization's expectations of its employees
  - develop a Use Policy
  - rules and penalties
  - require user to acknowledge by signature
  - may require HR and union participation
- States the employee's rights
  - states level of personal privacy guaranteed
  - states how those rights will be protected

 hoytkesterson@earthlink.net

Crypto Security Policy statement

- States where the use of cryptography is mandated, recommended, or prohibited
  - states required strength of security methods
- States where key recovery is to be used
  - identifies the key recovery centers
  - identifies the conditions where key recovery is permitted
  - defines procedures to authorize and execute key recovery
  - identifies interface for external requests, e.g. by law enforcement
- States when key information can be discarded
  - one method to "discard" old information

 hoytkesterson@earthlink.net

Commerce and the digital signature

- Can digital signatures be accepted as a replacement for a hand-written signature?
- The American Bar Association developed the Digital Signature Guidelines
- States are developing legislation
- US Congress passed the Electronic Signatures in Global and National Commerce Act in June 2000
  - may override state laws
- European Union Electronic Signature Act
- ABA currently developing PKI Evaluation Guidelines
- Some confusion in terminology
  - » electronic signature
  - » secure electronic signature
  - » digital signature

hoytkesterson@earthlink.net

Federal Electronic Signature Act

- E-sign act does not make an electronic signature “legal”
- No contract, signature, or record shall be denied legal effect solely because it is in electronic form.
  - parties must agree, i.e. opt in
  - notices such as eviction and utility cut-off are excluded
- Technology neutral
  - Electronic signature, not digital signature
  - Are more explicit state laws preempted?
- Effective 1 October 2000
- President Clinton digitally signed bill in Independence Hall on 30 June 2000
  - used a smartcard containing certificates and private key
  - certificate issued by ACES (1st issued and used)
    - » Access Certificates for Electronic Services
    - » Government-wide public key infrastructure
    - » http://hydra.gsa.gov/aces/

 hoytkesterson@earthlink.net

State activity

- Many states examining their statutes for requirement of “writing” or “signed”
  - Illinois found over 3000
- States are passing laws and/or regulations
  - see http://www.abanet.org/scitech/ec/isc/digital.html
- Early adopters, e.g. Utah and Washington, are technology specific
  - digital signature
  - licensed CAs and repositories
  - in Arizona legislation one will find “asymmetric cryptosystem means an algorithm or series of algorithms that provide a secure key pair for a digital signature”
- Many now becoming technology *neutral*
  - allow electronic records and signatures

 hoytkesterson@earthlink.net

Arizona activity

- Arizona Electronic Signature Act
  - "An electronic signature shall be unique to the person using it, shall be capable of reliable verification and shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated."
  - both technology neutral and technology specific
- Arizona Electronic Notary Act
  1. allows notaries to notarize physically presented electronic documents
  2. if a notary operates a Registration Authority, signatures supported by a certificate from that RA and by a timestamp from a recognized provider are considered notarized as if physically presented to that notary
- Arizona Electronic Transactions Act (AETA)
  - addresses electronic transactions — records, signing, notarization, and consumer protection
  - covers business, commercial, and government transactions
- Details at www.sos.state.az.us/pa
  - Secretary of State office sets policy and procedures for use within state government and for use when interacting with state government

 hoytkesterson@earthlink.net

Other activity

- The United Nations Commission on International Trade Law (UNCITRAL) is developing "Uniform Rules on Electronic Signatures"
- Many countries are developing regulation and legislation
  - e.g. Canada, UK, Colombia
  - European Community framework for electronic signatures
    - » informal final version
    - » http://europa.eu.int/comm/dg15/en/media/sign/99-915.htm.
- US government also developing rules for internal use and to promote national interoperation
  - NIST defining national PKI
  - many agencies planning deployment

 hoytkesterson@earthlink.net

PKI Evaluation Guidelines (PEG)

- Being developed by the American Bar Association Information Security Committee
- Assessment/accreditation of PKI components
- Obligation and rights of the parties involved
  - from Certification Practice Statement
  - from Certificate Policy
- Liabilities of the parties
- Operational requirements
- Audit

 hoytkesterson@earthlink.net

What will be “best practice”?

- Assurance that crypto functions supporting a transaction are correctly executed
- If a transaction is challenged, all components involved will be examined and challenged
  - is the CA operated according to an accepted standard of care?
  - did the subscriber protect the private key?
  - are there acceptable crypto services on the subscriber's platform?
  - did the relying party system perform properly?
- Is an audit necessary to prove compliance
  - how often?
  - just the CA? or other components such as subscriber software?
- The *best practice* bar is continually being raised

 hoytkesterson@earthlink.net

The current PKI scene

- Relying party software that can conform to a policy doesn't exist yet
- Most use currently is in browsers
  - Hence the appearance of human readable text
- "Battle" between hierarchical CA and cross certified CA approaches
- Difficult to insure the parties in a PKI
  - No history
  - Some states have capped liability
- Somewhere in the future
  - Open EDI - "I need a thousand widgets by 15 June 1999"
  - A sentient cash register will implement the policy contained in the certificate, e.g. display, according to locale, the terms of the sale on the display for the customer

 hoytkesterson@earthlink.net

The conundrum

The wonderful thing about personal computers is that

You can do almost anything with them

The horrible thing about personal computers is that

You can do almost anything with them

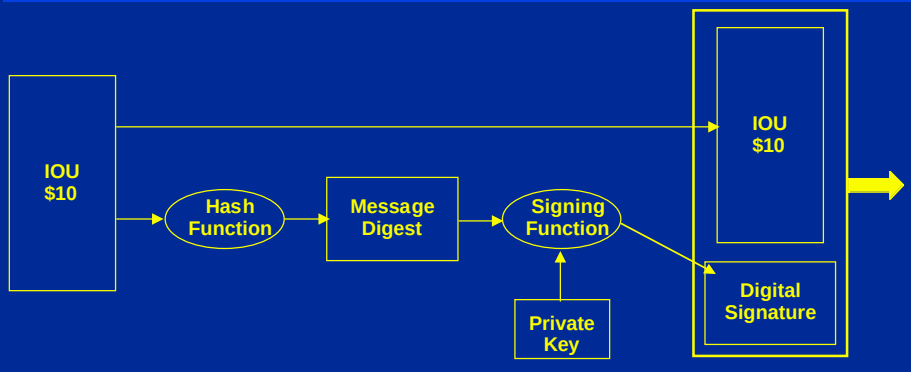
 hoytkesterson@earthlink.net

A problem

- A recent Trojan Horse attack sent email from a target's email system to everyone in the target's address book
- The attack used services that were provided to make life easier for the user
  - write a form letter
  - automatically tailor it for each person in the address book
  - automatically email it to each person in the address book
- An attractive new service? — let's automatically digitally sign each message
- If a message digitally signed unintentionally by a purchasing agent has as a subject "hello sexy", it's an irritation
- If a message digitally signed unintentionally by a purchasing agent has as a subject "purchase order", it's a problem

 hoytkesterson@earthlink.net

Signing a message



- If performed properly we have confidence
  - that if the sent message is changed, it will be detected
  - that the sent message could have been signed by no other
  - that the message was the one the signer wanted to send
  - that the message will be handled according to the constraints specified in the associated certificate

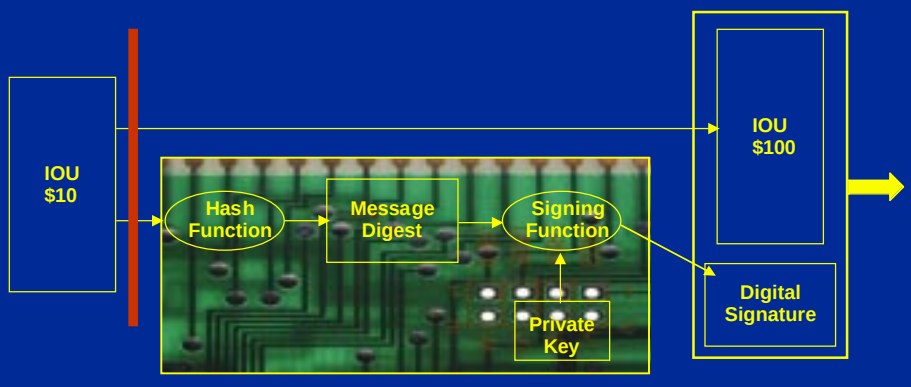
 hoytkesterson@earthlink.net

The vulnerabilities

- Soft is the key element in the term *soft*ware
- A program can be modified to do the wrong thing
- Routine libraries, e.g. a hash routine, can be suborned
- Even if routines are protected, e.g. in a smartcard
  - standard API calls can be intercepted
  - hidden calls can be found and modified
- These modifications are probably easier to accomplish than breaking the crypto-system
- Signing systems can be compromised in ways that would allow a message to be modified before it is signed
- Verifying systems can be compromised in ways that would ensure that all or selected signatures pass
  - routines are modified
  - bad "trusted CAs" are configured
- Identical problems and more for point-&-click over SSL

 hoytkesterson@earthlink.net

Find the weak link



 hoytkesterson@earthlink.net

Some engineering solutions

- Demand explicit OK from user for each signing
- Automatic signing facilities use only those certificates whose policy permit their use for automatic signings
- Move routines to protected environments, e.g. smartcard
  - enables focus on remainder of code, hopefully smaller and less complex
  - simplifies and reduces areas of audit
- Deploy more robust operating systems
  - utilize hardware memory protection functions

Practically perfect in every way
is difficult to achieve

 hoytkesterson@earthlink.net

What to Do?

- Market pressure should force systems to become better
- Enterprise systems should adhere to a policy
  - the Identrus model mandates approved software
  - non-conforming systems may be detectable
  - audit signing and relying-party systems
  - but users will still do stupid things, e.g. the *nakked wife* syndrome
- May be able to control internal and B2B systems
  - audit signing and verifying systems
- What about consumer systems?
- An *internet appliance* may be the answer
  - upgradable? then it may be subornable

Even if the system did only what it was supposed to do
There are other problems, for example...

 hoytkesterson@earthlink.net

Was the signer forced in any way?

A technical solution to determine state of mind seems far away

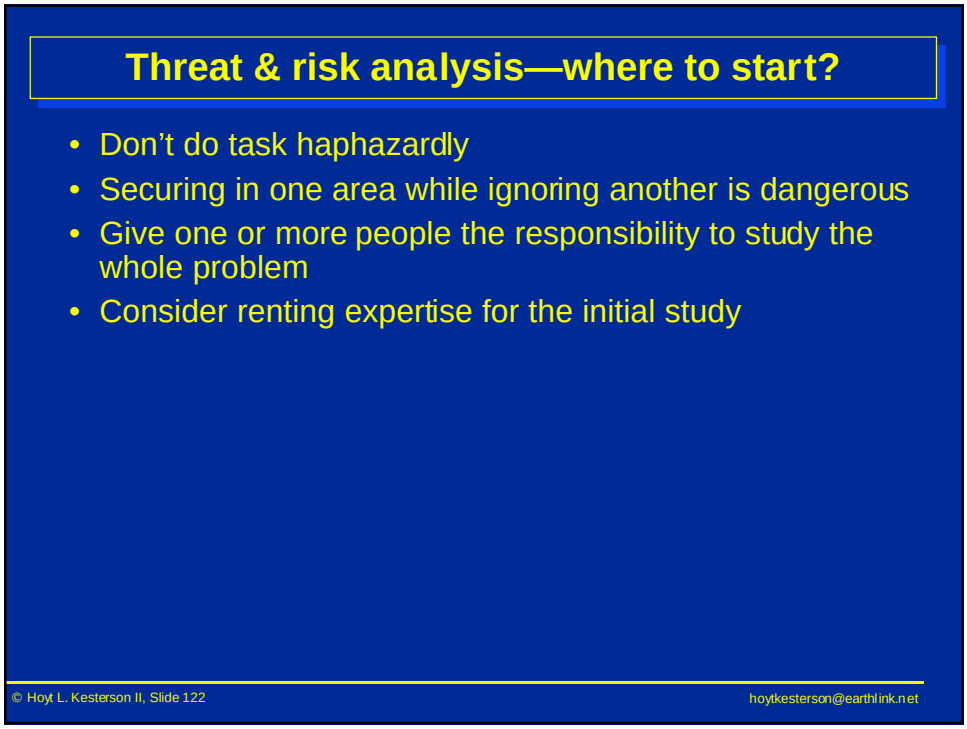
 hoytkesterson@earthlink.net

The lawyers will figure this out

- Lawyers work with systems that aren't perfect
- Judicial decisions frequently "raise the bar"
- There is a spectrum of approaches
- The system has been selecting appropriate technology for a long time
  — sign with ink, not pencil
- It is a risk management decision

 hoytkesterson@earthlink.net


© Hoyt L. Kesterson II, Slide 121
hoytkesterson@earthlink.net


Threat & risk analysis—where to start?
• Don't do task haphazardly
• Securing in one area while ignoring another is dangerous
• Give one or more people the responsibility to study the whole problem
• Consider renting expertise for the initial study
© Hoyt L. Kesterson II, Slide 122
hoytkesterson@earthlink.net

What does one look at?

- Everything!
- Not enough to secure your mainframe if someone can masquerade as your departmental systems
- Not enough to secure communication with the departments if they can be penetrated
- Not enough to secure the software of departmental systems if they are not physically secure
- Irresponsible or uninformed user actions weaken the strongest security
- Make an informed choice of where to invest your security dollar
- Balance is the key — Everyone must participate.

The security review process

- You have to ask questions
  - what is your mission and how do you go about doing it?
    - » how are you changing it?
  - the threats—what can go wrong?
    - » examine hardware, software, and network configurations
    - » examine the administrative processes
  - the risks—what if something does go wrong?
    - » a minor irritation
    - » embarrassment
    - » resources misappropriated
    - » operational delay
    - » inability to perform mission
    - » punitive legal action
- Rank the risks
- Deploy solutions to counter the threat or eliminate the risk
  - confidence in the correctness and robustness of the product

Security is an ongoing activity

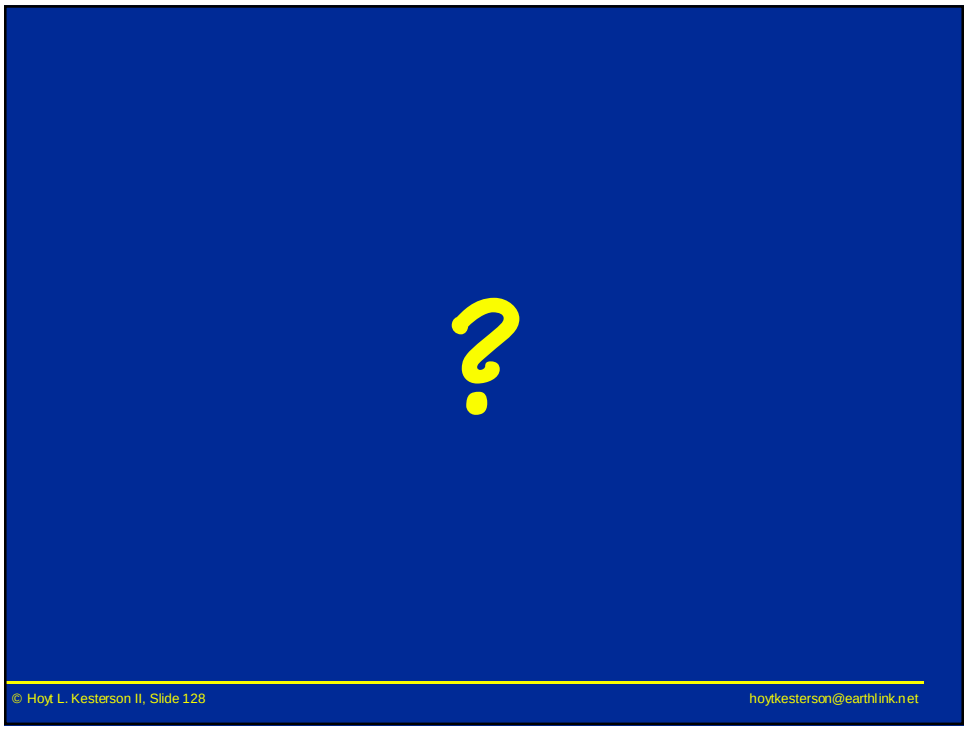
- Cannot deploy it and forget it
- Appoint a security officer
  - empowered by senior management
  - knowledgeable about IT security
  - technically capable
- Monitor compliance to policy
- Examine audit records for suspicious activity
- Keep up to date on discovered vulnerabilities and new threats
- As you change the enterprise, re-evaluate your security
- Security must help the enterprise, not hinder it

 hoytkesterson@earthlink.net

Perfect implementation of perfect algorithms is not the goal

The goal is acceptable risk

 hoytkesterson@earthlink.net


?
© Hoyt L. Kesterson II, Slide 128
hoytkesterson@earthlink.net